Internet Commerce Coalition

Response to NTIA Big Data Request for Comments

I. Introduction

The Internet Commerce Coalition ("ICC") appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration ("NTIA") request for comment on its "Big Data" review. The ICC is comprised of leading Internet and e-commerce companies and trade associations. We work to promote balanced, reasonable and workable rules and standards governing liability, privacy and security relating to the Internet.

Our Coalition has supported the Administration's White Paper and Privacy Bill of Rights[1]. We also strongly support the decision to review the Privacy Bill of Rights framework in light of big data applications in order to achieve the combination of privacy protection, flexibility and respect for context that characterized the 2012 articulation of the Privacy Bill of Rights.

II. Response to the Questions in the Request for Comment

Q. 1: It is important to acknowledge at the outset that there may be trade-offs between privacy protections and innovative, beneficial uses of big data.[2] The Privacy Bill of Rights should strike a balance and should not attempt to codify best practices that will doubtless continue to evolve as innovation both in data uses and privacy practices continues.

Qs 2-4. We agree in principle with bolstering and in some cases substituting a responsible use framework with notice and choice in the big data context. The nature of big data uses makes advance notice and consent impractical in many circumstances – particularly for data that have been collected before the use is decided upon.

We further believe that the data destruction requirements of the Bill of Rights could undermine innovation in big data, and should be reviewed in this context, particularly as to data that have been de-identified.

On the other hand, just-in-time notice, where it reasonably can be provided, may be useful in some contexts -- for example, for sharing location data with third parties,, which may be deemed more sensitive and from which individuals may be identified more easily. In this

[1] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[2] *See, e.g.*, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, 11-12 (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf hereinafter the "White House Big Data Report").

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000

regard, just-in-time notice could be encouraged as an alternative to in-advance notice as a useful tool to allow choices in big data environments.
On the other hand, just-in-time notice is impractical in many circumstances – for example when individuals have been de-identified, or when the use is obvious or otherwise fits the context principle. Determining when to do just-in-time notice requires an awareness of the need to avoid over-notification and notice fatigue for users.

Much like the use-based framework of the Fair Credit Reporting Act ("FCRA"), a responsible use framework can avoid potential privacy and discrimination harms from data applications, leaving room for innovation while protecting against potential downsides of improper data uses.

Q. 12: The potential discriminatory effects of big data analytics that would deny consumers access to credit/employment/insurance and other important benefits are a very serious issue. Fortunately, the FCRA already prohibits use of consumer data for these purposes without notice and opt-in consent, and the Federal Trade Commission ("FTC") has brought a number of cases against big data uses that violated the FCRA.[3]

Furthermore, strong U.S. anti-discrimination laws bar discriminatory effects with regard to fair housing, fair lending, employment discrimination and in federal programs.[4] It should certainly be no defense that a discriminatory effect was caused by reliance on big data analytics tools.

By contrast, advertising and marketing uses of big data analytics do not give rise to the same concerns, unless used in a way that that discriminates against data subjects in violation of civil rights or other laws. It is that *use*, rather than the methodology or technology, that may create risk of discrimination.

Qs. 7-11. De-identification is a helpful step for privacy protection that should be encouraged, not rejected, because of theoretical risk of re-identification, particularly when re-

[3] *See, e.g.*, Federal Trade Commission, *Two Data Brokers Settle FTC Charges That They Sold Consumer Data Without Complying With Protections Required Under the Fair Credit Reporting Act* (Apr. 9, 2014), http://www.ftc.gov/news-events/press-releases/2014/04/two-data-brokers-settle-ftc-charges-they-sold-consumer-data. For a more complete overview and listing of FTC FCRA enforcement actions go to http://www.ftc.gov/news-events/media-resources/consumer-finance/credit-reporting.

[4] *See, e.g.*, Fair Housing Act, 42 U.S.C. §§ 3601-19 ("it shall be unlawful to deny any person access to or membership or participation in any multiple-listing service, real estate brokers' organization or other service, organization, or facility relating to the business of selling or renting dwellings, or to discriminate against him in the terms or conditions of such access, membership, or participation, on account of race, color, religion, sex, handicap, familial status, or national origin"), *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2009-title42/html/USCODE-2009-title42-chap45-subchapI.htm.

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000

identification is prohibited by internal policies or by contracts with third parties, as applicable.[5] To do otherwise would be to remove incentives to de-identify data and to ignore context.

There is clearly some research, highlighted in the President's Council of Advisors on Science and Technology ("P-CAST") report titled "Big Data and Privacy", showing that identification or re-identification of de-identified data is possible.[6] However, it is also clear that data from publicly released data sets are much more likely to be re-identified than are privately held ones. The fact that something can happen does not mean that it will happen, much less that it will cause harm to individuals.

Importantly, this issue has already been addressed and "solved" in the March 2012 FTC report titled "Protecting Consumer Privacy in an Era of Rapid Change", which offers a clear, very useful framework for protecting de-identified data, including applying internal rules and binding by contract third parties who receive the data from re-identifying it.[7] Failure to honor that commitment could itself be the subject of enforcement actions, and the Administration could review FTC and other authorities to pursue such conduct as an unfair or deceptive trade practice.

Most importantly, in contrast to discrimination against protected classes, we believe that the actual "risks" posed by re-identification that are noted in the P-CAST report are quite limited and can be fully addressed through a responsible use framework that guards against harmful uses of big data analytics. As the FTC noted in its March 2012 staff report, internal rules and contractual prohibitions against third parties re-identifying data are also effective. More generally, it is important to understand these "identification risks" in practical terms and to put into context the very low level of concrete risk from identification/re-identification, when a responsible use framework is in place to prevent misuse of those data.

---

[5] *See* Ann Cavoukian and Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* (June 16, 2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identification_ITIF1.pdf.

[6] Report to the President, President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, 38-39 (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[7] FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, 21 (Mar. 2012), ("First, the company must take reasonable measures to ensure that the data is de-identified. This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device. Consistent with the Commission's approach in its data security cases,108 what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant. Thus, for example, whether a company publishes data externally affects whether the steps it has taken to de-identify data are considered reasonable. The standard is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified."), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000

Internet Commerce Coalition

Q. 13. We believe that internal review committees of data uses can in some cases be an important part of privacy by design and an appropriate way to screen big data uses. Our members already conduct these reviews and believe that they are well adapted to screen for potential downsides of big data uses as regards privacy or discrimination against protected classes of individuals. However, there needs to be more policy development by stakeholders on when a company should use such a committee (because using them for every data use would be unworkable). Further, smaller companies including many app developers may not have the capacity to have a committee, which likewise merits further consideration by stakeholders.

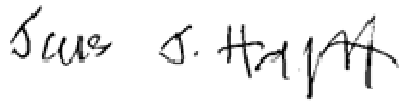
Q. 16. We do not believe that a National Institute of Standards and Technology ("NIST") privacy risk framework would be particularly helpful given the many best practice guidance documents on privacy that already exist and the considerable clarity in the existing privacy bill of rights document. To the extent that there are technical standards questions to resolve, NIST may have a role, but a privacy risk framework involves normative judgments that are not particularly susceptible to productive NIST workshops.

Qs.14 and 15. Differential privacy and privacy risk meta-data tags that would specify consumers' across-the-board privacy preferences as metadata likely would not undermine beneficial uses of big data. This is because, as some proponents of differential privacy concede, data sets would be compromised before being used. Furthermore, with regard to privacy preference tags, the very nature of big data uses is that they are often unforeseen at the time a consumer is asked for his or her preference, so the value proposition cannot be presented at the time. In fact, privacy tags are a form of a consent regime. In the particular case of sensitive data that could cause harm to individuals if disclosed – for example, personally identifiable financial account information or health treatment data – these or other measures may be appropriate. However, as an across-the-board recommendation, as we understand them, these measures costs would outweigh their benefits.

Conclusion

For all these reasons, we support: (1) adding responsible use to the Privacy Bill of Rights framework as it applies to big data uses; (2) using just-in-time notice in some contexts; (3) relaxing the data destruction principle, where doing this would reduce the utility of big data applications; and (4) continuing recognition of de-identification exceptions where de-identification controls meet the de-identification criteria set forth in the March 2012 FTC report ("Protecting Consumer Privacy in an Era of Rapid Change").

Respectfully submitted,



500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000

Jim Halpert, General Counsel

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000